advenica

Traceability and Security Logging

Centralised logging in security-sensitive systems involves an enhanced risk of attacks. To reduce the risks, a solution is needed that protects both log data and all connected systems.

Challenge

Create Secure Centralised Logging

Most IT systems generate logs that enable troubleshooting and traceability. To benefit the most from such logs, it is important to combine logs from as many systems as possible in one chronological list. If you have security-sensitive or zoned systems and want to implement centralised logging, you need to resolve an inherent goal conflict. Logging benefits from having one shared system for all zones/subsystems, but a shared system also increases the risk of attacks.

1. The risk of the log system being contaminated with confidential data

If any of the zones contains confidential data, there is a risk of the log system also being contaminated with confidential data. If this happens, the need for protection increases as the zone from which the data comes, and also the log system, must be protected against leakage of the confidential data.

2. The risk of the log system being used as a stepping stone for attacks

If the log server is connected to several zones, it becomes an attractive intermediate target for attacking a system in another zone via the log server.

3. The risk of the log system being used for reconnaissance ahead of future attacks

The log system makes it possible to draw conclusions about which events are visible. An attacker can adapt their method of attack and thus reduce the risk of detection.

4. The risk of the log system being attacked to cover up the tracks of an attack

If an attacker can access the log system, they can corrupt or delete log data, affecting the reliability of log data. There is also a risk of log data being deleted or corrupted even before it reaches the log system.

Solution

Unidirectional Data Flow

All the zones that supply log data are protected with one data diode each. The data flow is made unidirectional towards the log system. A shared log system can therefore be used regardless of the number of zones supplying data to the log system. If any of the zones contains confidential data, either the log system must be protected at the appropriate confidentiality level, or the log data from such a zone must be filtered so that the log system is not contaminated with confidential data. However, this can lead to the value of the log data decreasing as free text data often needs to be filtered out, which may make it more difficult to interpret log data.

- The diodes make it impossible to use the log system as a stepping stone (2).
- The diodes make it easy to protect the log system so that no unauthorised person can access the data (1,3).
- It is much more difficult for an attacker to cover their tracks after an attack (4).
- It is also possible to encrypt the connection to the log server to prevent corruption of log data (4).

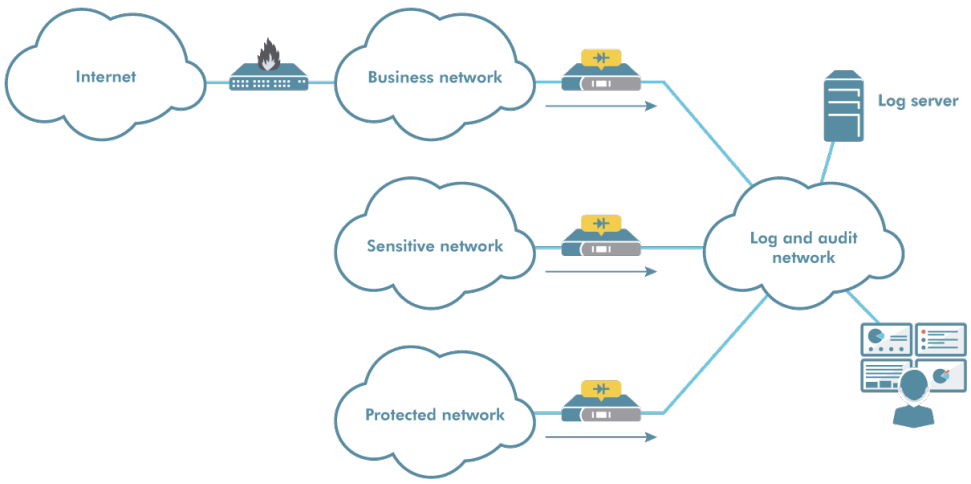
Advantages

Protect the Collection of Log Data

Using data diodes to protect the collection of log data, you achieve very good protection:

- It is impossible to carry out attacks from the log system on any of the zones.
- You can use a shared log system regardless of the number of zones connected. This avoids the additional costs of having to maintain several log systems in parallel.
- You can easily shield and protect the log system so that no unauthorised person can access its contents.
- Data diodes means simplified security analysis (and thus simplified commissioning) and meet extremely strict requirements from bodies such as supervisory authorities.

To read more about our data diodes, please visit advenica.com.



advenica

Advenica provides expertise and world-class high assurance cybersecurity solutions for critical data in motion up to Top Secret classification. We enable countries, authorities and companies to raise information security and digitalise responsibly. Founded in 1993, we are EU approved to the highest level of security. Our unique products are designed, developed and manufactured in Sweden.

Read more at advenica.com

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED